rbd - Bug #40368
[rbd-mirror] image sync can crash when updating progress
06/14/2019 03:11 PM - Jason Dillaman

Status: Resolved
Priority: Normal
Assignee: Jason Dillaman
Category: Target version:

% Done: 0%
Spent time: 0.00 hour
Assignee: Jason Dillaman

Description
The invocation of "m_copied_objects.top()" is not guarded so it might be invoked on an empty heap, resulting in an assertion failure.

```
#0 0x00007fffebe74c93f in raise () from /lib64/libc.so.6
#1 0x00007fffebe736c95 in abort () from /lib64/libc.so.6
#2 0x0000555555577008 in std::replacement_assert (__file=__file@entry=0x55555551af78 "/usr/include/c++/8/bits/stl_queue.h", __line=__line@entry=582,
__function=__function@entry=0x5555555c1b0c0 <std::priority_queue<unsigned long, std::vector<unsigned long, std::allocator<unsigned long>, std::greater<unsigned long>>>::top() const::__PRETTY_FUNCTION__ > std::priority_queue<Tp, _Sequence, _Compare>::const_reference std::priority_queue<Tp, _Sequence, _Compare>::top () const [with _Tp = long unsigned int; _Sequence = std::vector<long unsigned int>::_Co...,
__condition=__condition@entry=0x5555555b61e8 ".builtin_expect(!this->empty(), true)"") at /usr/include/c++/8/x86_64-redhat-linux/bits/c++config.h:2391
#3 0x000055555559f3bf in std::priority_queue<unsigned long, std::vector<unsigned long, std::allocator<unsigned long>, std::greater<unsigned long>>>::top (this=0x7fff440b0318)
at /usr/include/c++/8/bits/stl_iterator.h:783
#4 librbd::deep_copy::ImageCopyRequest<librbd::ImageCtx>::finish (this=this@entry=0x7fff740f37e0, r=r@entry=-2) at /usr/include/c++/8/ext/new_allocator.h:86
#5 librbd::deep_copy::ObjectCopyRequest<librbd::ImageCtx>::handle_read_from_parent (this=this@entry=0x7fff740f37e0, r=r@entry=0) at /usr/include/c++/8/bits/stl_map.h:463
#6 librbd::deep_copy::ObjectCopyRequest<librbd::ImageCtx>::send_read_from_parent (this=0x7fff740f37e0) at /usr/src/debug/ceph-14.2.1-385.g4ae8136.el8cp.x86_64/src/common/RWLock.h:123
#7 librbd::deep_copy::object_copy_request (this=0x7fff740f37e0) at /usr/src/debug/ceph-14.2.1-385.g4ae8136.el8cp.x86_64/ceph-14.2.1-385.g4ae8136.el8cp.x86_64/src/librados/AioCompletionImpl.h:167
```

Reviewed:

Affected Versions:
ceph-qa-suite:
Pull request ID: 28559
Crash signature (v1):
Crash signature (v2):
Related issues:
Copied to rbd - Backport #40379: nautilus: [rbd-mirror] image sync can crash ... Resolved
Copied to rbd - Backport #40380: mimic: [rbd-mirror] image sync can crash when updating progress Resolved

History
#1 - 06/14/2019 05:40 PM - Jason Dillaman
- Status changed from In Progress to Fix Under Review
- Pull request ID set to 28559

#2 - 06/14/2019 05:42 PM - Jason Dillaman
- Subject changed from [rbd-mirror] image sync can crash due to out-of-order object copying to [rbd-mirror] image sync can crash when updating progress

#3 - 06/15/2019 09:05 AM - Mykola Golub
- Status changed from Fix Under Review to Pending Backport

#4 - 06/15/2019 09:43 AM - Nathan Cutler
- Copied to Backport #40379: nautilus: [rbd-mirror] image sync can crash when updating progress added

#5 - 06/15/2019 09:43 AM - Nathan Cutler
- Copied to Backport #40380: mimic: [rbd-mirror] image sync can crash when updating progress added

#6 - 10/08/2019 05:32 PM - Nathan Cutler
- Status changed from Pending Backport to Resolved

While running with --resolve-parent, the script "backport-create-issue" noticed that all backports of this issue are in status "Resolved" or "Rejected".